

FILED

JUN 28 2023

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
at KNOXVILLE

Clerk, U. S. District Court
Eastern District of Tennessee
At Knoxville

IN THE MATTER OF THE SEARCH OF:
A Mobile Device in the Custody or Control
of Michael Asbury

Case No. 3:23-mj-
Magistrate Judge

2124

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Jessi A. Mann, being first duly sworn, hereby depose and state as follows:

AGENT BACKGROUND

1. Your affiant, Jessi Ann Mann, is an FBI Special Agent assigned to the FBI Knoxville Division. In my duties as a special agent, I am assigned to Joint Terrorism Task Force (JTTF). Currently, I am tasked with investigating criminal activity in and around the Capitol grounds on January 6, 2021. As a Special Agent, I am authorized by law or by a Government agency to engage in or supervise the prevention, detection, investigation, or prosecution of a violation of Federal criminal laws.

2. The facts in this Affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies or is based on a review of various documents, records, and reports. Because this Affidavit is submitted for the limited purpose of establishing probable cause, it does not contain every fact known by me or the FBI. The time stamps, dates, and times listed in this Affidavit should be read as "on or about."

PURPOSE OF AFFIDAVIT

3. I make this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search (1) a cellphone, bearing MSISDN: 8657652423, IIMEI Number 356694099258140 and/or any successor cellphone ("Subject Device") recovered

from Michael ASBURY. The **Subject Device** is described in the following paragraphs and in Attachment A. The items and evidence to be seized are further described in Attachment B.

4. According to records from the Tennessee Department of Motor Vehicles (DMV), subject MICHAEL ASBURY is 43 years old, and his primary residence is located in Knoxville, Tennessee.

5. Based on my training and experience and the facts as set forth in this Affidavit, there is probable cause to believe that ASBURY and others have committed violations of Title 18, United States Code, Section 231(a)(3), and 1752(a)(1)(2); and Title 40, United States Code, Sections 5104(e)(2)(D)(F) (collectively, the “**Target Offenses**”). There is also probable cause to search the **Subject Device** described in Attachment A for evidence, fruits, or instrumentalities of these crimes further described in Attachment B.

PROBABLE CAUSE

Background: Events at the U.S. Capitol on January 6, 2021

6. U.S. Capitol Police (USCP), the FBI, and assisting law enforcement agencies are investigating a riot and related offenses that occurred at the United States Capitol Building, located at 1 First Street, NW, Washington, D.C., 20510 at latitude 38.88997 and longitude -77.00906 on January 6, 2021.

7. At the U.S. Capitol, the building itself has 540 rooms covering 175,170 square feet of ground, roughly four acres. The building is 751 feet long (roughly 228 meters) from north to south and 350 feet wide (106 meters) at its widest point. The U.S. Capitol Visitor Center is 580,000 square feet and is located underground on the east side of the Capitol. On the west side of the Capitol building is the West Front, which includes the inaugural stage scaffolding, a variety of open concrete spaces, a fountain surrounded by a walkway, two broad staircases, and multiple

terraces at each floor. On the East Front are three staircases, porticos on both the House and Senate side, and two large skylights into the Visitor's Center surrounded by a concrete parkway. All of this area was barricaded and off limits to the public on January 6, 2021.

8. The U.S. Capitol is secured 24 hours a day by USCP. Restrictions around the U.S. Capitol include permanent and temporary security barriers and posts manned by USCP. Only authorized people with appropriate identification are allowed access inside the U.S. Capitol.

9. On January 6, 2021, the exterior plaza of the U.S. Capitol was closed to members of the public.

10. On January 6, 2021, a joint session of the United States Congress convened at the U.S. Capitol. During the joint session, elected members of the United States House of Representatives and the United States Senate were meeting in separate chambers of the U.S. Capitol to certify the vote count of the Electoral College of the 2020 Presidential Election, which took place on November 3, 2020 ("Certification"). The joint session began at approximately 1:00 p.m. Eastern Standard Time (EST). Shortly thereafter, by approximately 1:30 p.m. EST, the House and Senate adjourned to separate chambers to resolve a particular objection. Vice President Mike Pence was present and presiding, first in the joint session, and then in the Senate chamber.

11. As the proceedings continued in both the House and the Senate, and with Vice President Mike Pence present and presiding over the Senate, a large crowd gathered outside the U.S. Capitol. As noted above, temporary and permanent barricades were in place around the exterior of the U.S. Capitol building, and USCP were present and attempting to keep the crowd away from the Capitol building and the proceedings underway inside.

12. At around 1:00 p.m. EST, known and unknown individuals broke through the police lines, toppled the outside barricades protecting the U.S. Capitol, and pushed past USCP and supporting law enforcement officers there to protect the U.S. Capitol.

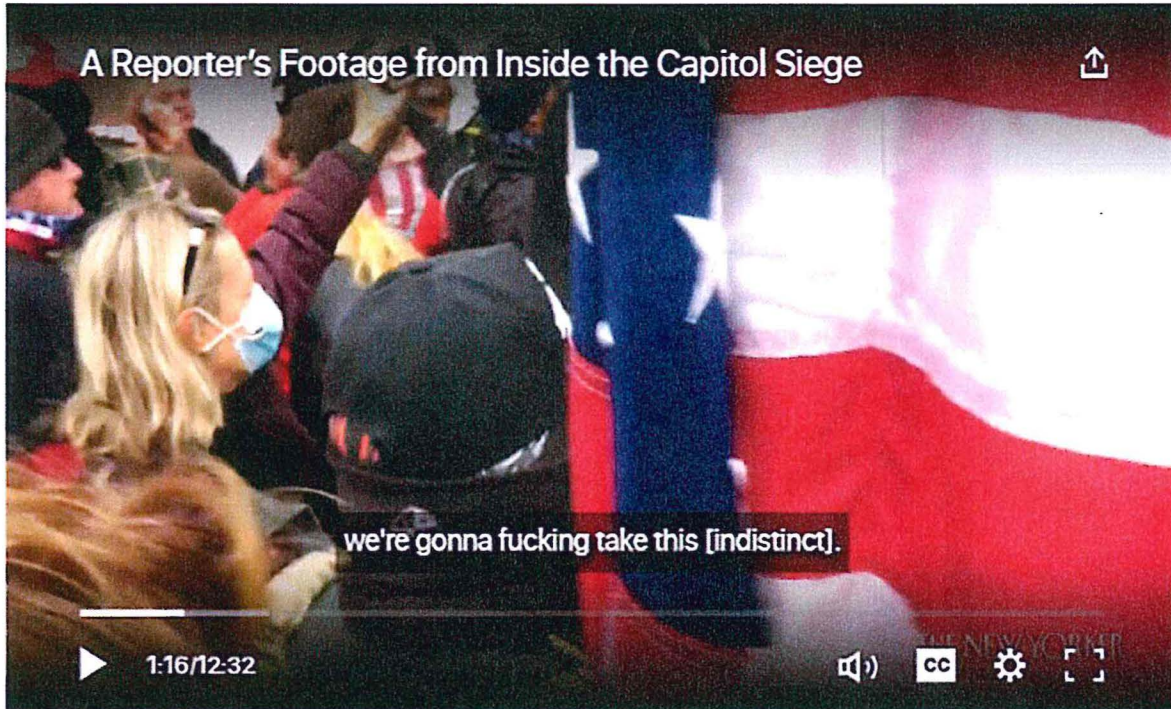
13. At around 1:30 p.m. EST, USCP ordered Congressional staff to evacuate the House Cannon Office Building and the Library of Congress James Madison Memorial Building in part because of a suspicious package found nearby. Pipe bombs were later found near both the Democratic National Committee and Republican National Committee headquarters.

14. Media reporting showed a group of individuals outside of the Capitol chanting, "Hang Mike Pence." I know from this investigation that some individuals believed that Vice President Pence possessed the ability to prevent the certification of the presidential election and that his failure to do so made him a traitor.

15. At approximately 2:00 p.m. EST, some people in the crowd forced their way through, up, and over the barricades and law enforcement. The crowd advanced to the exterior façade of the building. The crowd was not lawfully authorized to enter or remain in the building and, prior to entering the building, no members of the crowd submitted to security screenings or weapons checks by U.S. Capitol Police Officers or other authorized security officials. At such time, the certification proceedings were still underway and the exterior doors and windows of the U.S. Capitol were locked or otherwise secured. Members of law enforcement attempted to maintain order and keep the crowd from entering the Capitol.

16. Shortly after 2:00 p.m. EST, individuals in the crowd forced entry into the U.S. Capitol, including by breaking windows and by assaulting members of law enforcement, as others in the crowd encouraged and assisted those acts. Publicly available video footage shows an

unknown individual saying to a crowd outside the Capitol building, “We’re gonna fucking take this,” which your affiant believes was a reference to “taking” the U.S. Capitol.



17. Shortly thereafter, at approximately 2:20 p.m. EST, members of the United States House of Representatives and United States Senate, including the President of the Senate, Vice President Mike Pence, were instructed to—and did—evacuate the chambers. That is, at or about this time, USCP ordered all nearby staff, Senators, and reporters into the Senate chamber and locked it down. USCP ordered a similar lockdown in the House chamber. As the subjects attempted to break into the House chamber, by breaking the windows on the chamber door, law enforcement were forced to draw their weapons to protect the victims sheltering inside.

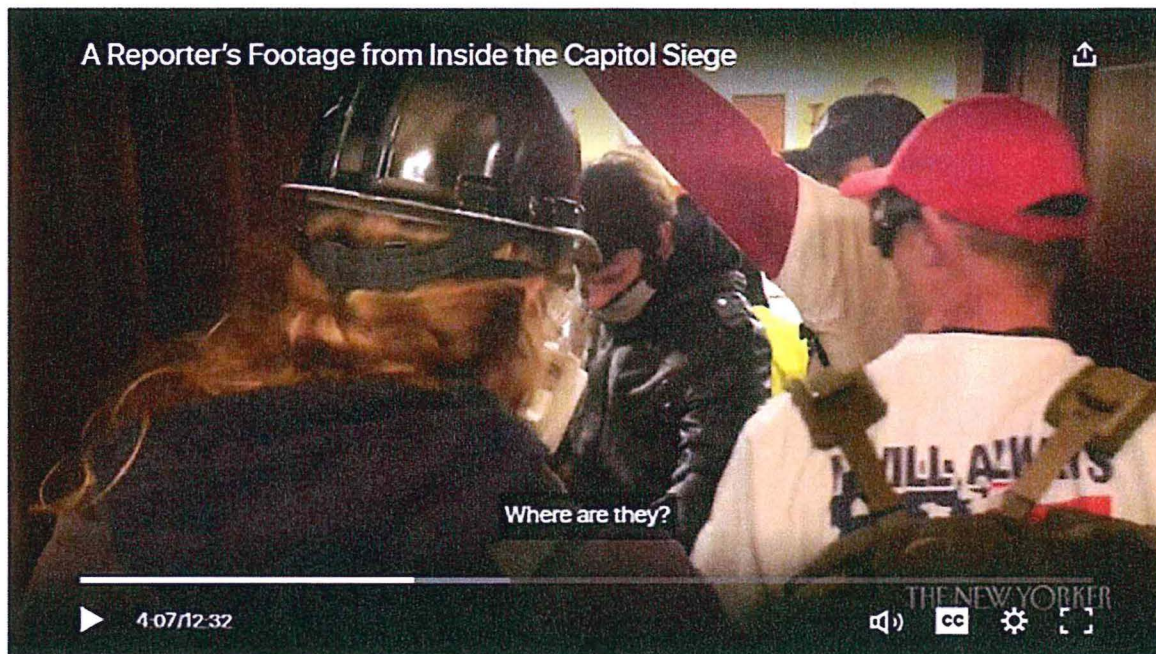
18. At approximately 2:30 p.m. EST, known and unknown subjects broke windows and pushed past USCP and supporting law enforcement officers forcing their way into the U.S. Capitol on both the west side and the east side of the building. Once inside, the subjects broke windows

and doors, destroyed property, stole property, and assaulted federal police officers. Many of the federal police officers were injured and several were admitted to the hospital. The subjects also confronted and terrorized members of Congress, Congressional staff, and the media. The subjects carried weapons including tire irons, sledgehammers, bear spray, and tasers. They also took police equipment from overrun police including shields and police batons. At least one of the subjects carried a handgun with an extended magazine. These actions by the unknown individuals resulted in the disruption and ultimate delay of the vote Certification.

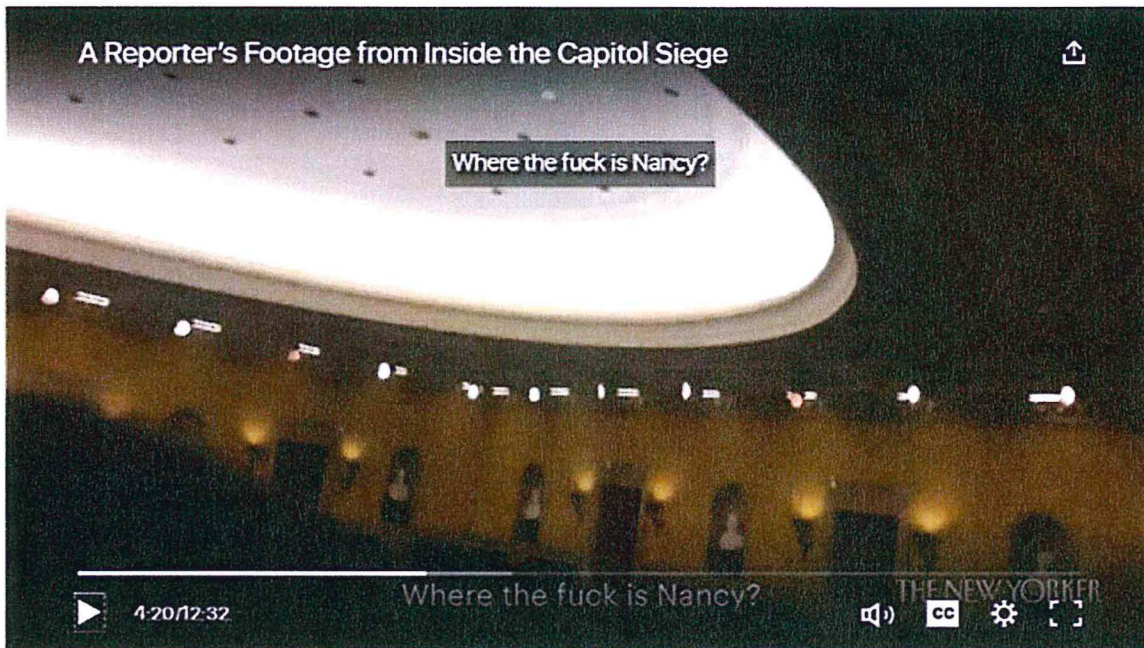
19. Also at approximately 2:30 p.m. EST, USCP ordered the evacuation of lawmakers, Vice President Mike Pence, and president pro tempore of the Senate, Charles Grassley, for their safety.

20. At around 2:45 p.m. EST, subjects broke into the office of House Speaker Nancy Pelosi.

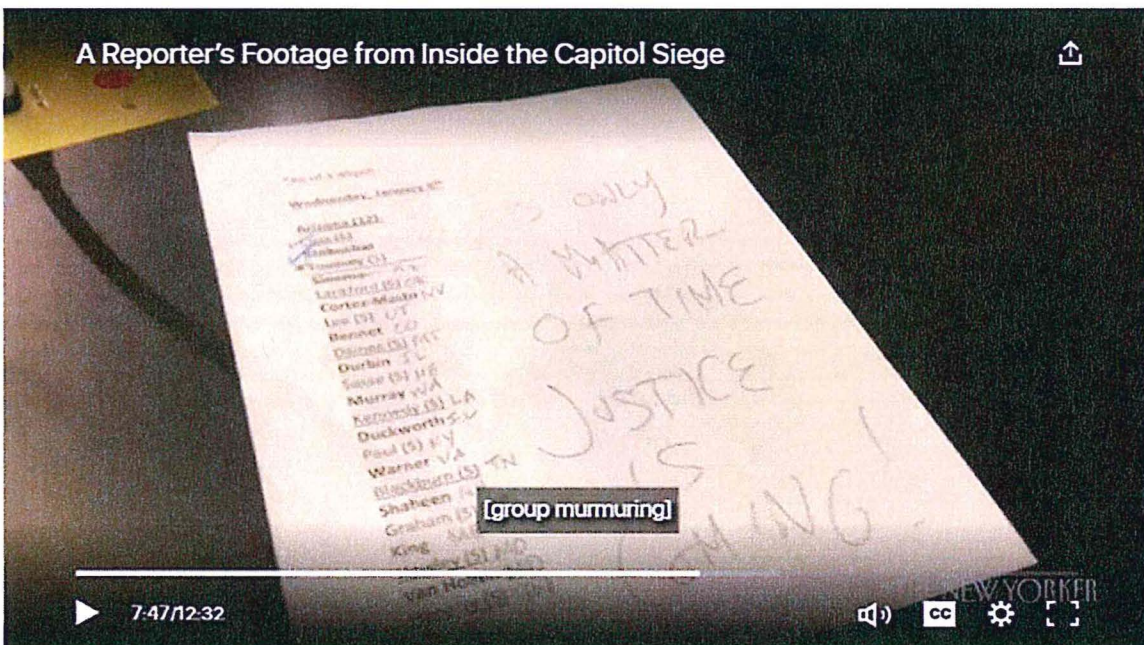
21. At around 2:47 p.m. EST, subjects broke into the United States Senate Chamber. Publicly available video shows an individual asking, “Where are they?” as they opened up the door to the Senate Chamber. Based upon the context, law enforcement believes that the word “they” is in reference to members of Congress.



22. After subjects forced entry into the Senate Chamber, publicly available video shows that an individual asked, “Where the fuck is Nancy?” Based upon other comments and the context, law enforcement believes that the “Nancy” being referenced was the Speaker of the House of Representatives, Nancy Pelosi.



23. One subject left a note on the podium on the floor of the Senate Chamber. This note, captured by the filming reporter, stated “A Matter of Time Justice is Coming.”



24. During the time when the subjects were inside the Capitol building, multiple subjects were observed inside the U.S. Capitol wearing what appears to be, based upon my training

and experience, tactical vests and carrying flex cuffs. Based upon my knowledge, training, and experience, I know that flex cuffs are a manner of restraint that are designed to be carried in situations where a large number of individuals are expected to be taken into custody.





25. At around 2:48 p.m. EST, DC Mayor Muriel Bowser announced a citywide curfew beginning at 6:00 p.m. EST.

26. At around 2:45 p.m. EST, one subject was shot and killed while attempting to break into the House chamber through the broken windows.

27. At about 3:25 p.m. EST, law enforcement officers cleared the Senate floor.

28. Between 3:25 and around 6:30 p.m. EST, law enforcement was able to clear the U.S. Capitol of all of the subjects.

29. Based on these events, all proceedings of the United States Congress, including the joint session, were effectively suspended until shortly after 8:00 p.m. EST the same day. In light of the dangerous circumstances caused by the unlawful entry to the U.S. Capitol, including the danger posed by individuals who had entered the U.S. Capitol without any security screening or weapons check, Congressional proceedings could not resume until after every unauthorized

occupant had left the U.S. Capitol, and the building had been confirmed secured. The proceedings resumed at approximately 8:00 pm after the building had been secured. Vice President Pence remained in the United States Capitol from the time he was evacuated from the Senate Chamber until the session resumed.

30. Beginning around 8:00 p.m. EST, the Senate resumed work on the Certification.

31. Beginning around 9:00 p.m. EST, the House resumed work on the Certification.

32. Both chambers of Congress met and worked on the Certification within the Capitol building until approximately 3:00 a.m. EST on January 7, 2021.

33. During national news coverage of the aforementioned events, video footage which appeared to be captured on mobile devices of persons present on the scene depicted evidence of violations of local and federal law, including scores of individuals inside the U.S. Capitol building without authority to be there.

34. Based on my training and experience, I know that it is common for individuals to carry and use their cell phones during large gatherings, such as the gathering that occurred in the area of the U.S. Capitol on January 6, 2021. Such phones are typically carried at such gatherings to allow individuals to capture photographs and video footage of the gatherings, to communicate with other individuals about the gatherings, to coordinate with other participants at the gatherings, and to post on social media and digital forums about the gatherings.

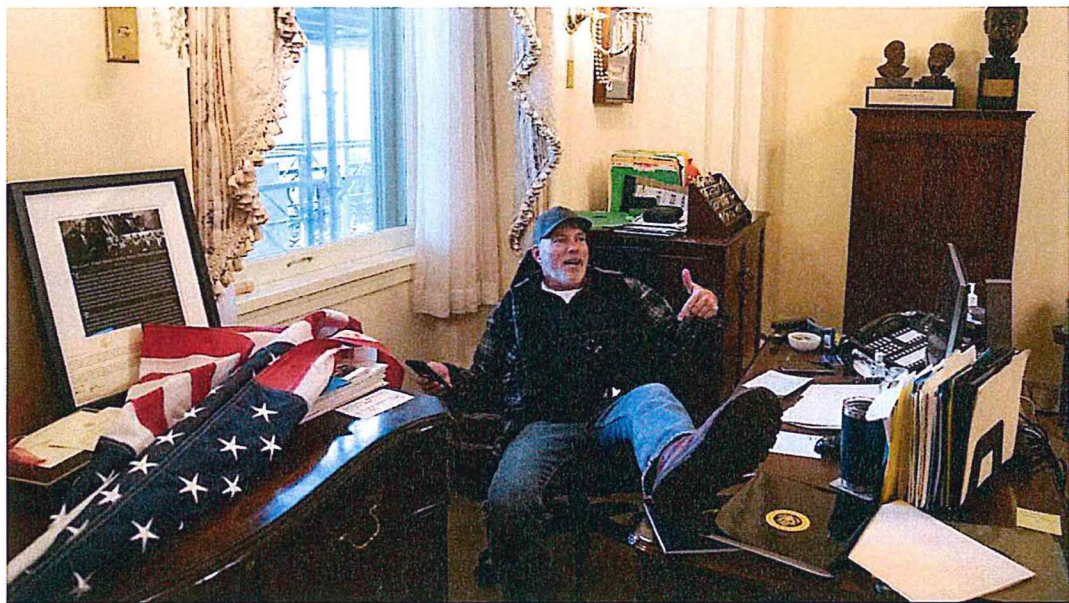
35. Many subjects seen on news footage in the area of the U.S. Capitol are using a cell phone in some capacity. It appears some subjects were recording the events occurring in and around the U.S. Capitol and others appear to be taking photos, to include photos and video of themselves after breaking into the U.S. Capitol itself, including photos of themselves damaging and stealing property. As reported in the news media, others inside and immediately outside the

U.S. Capitol live-streamed their activities, including those described above as well as statements about these activities.

36. Photos below, available on various publicly available news, social media, and other media show some of the subjects within the U.S. Capitol during the riot. In several of these photos, the individuals who broke into the U.S. Capitol can be seen holding and using cell phones, including to take pictures and/or videos:



¹ <https://losangeles.cbslocal.com/2021/01/06/congresswoman-capitol-building-takeover-an-attempted-coup/>



² <https://www.businessinsider.com/republicans-objecting-to-electoral-votes-in-congress-live-updates-2021-1>.

³<https://www.thv11.com/article/news/arkansas-man-storms-capitol-pelosi/91-41abde60-a390-4a9e-b5f3-d80b0b96141e>

IDENTIFICATION OF MICHAEL ASBURY

37. On January 13, 2021, an individual whose identity is known to the FBI, and who is identified herein as “Witness 1” submitted an online tip to the FBI, reporting that MICHAEL ASBURY of Knoxville, Tennessee, was a possible suspect in the riot at the United States Capitol. Witness 1 had viewed a video on ASBURY’s personal Facebook page depicting him on Capitol grounds on January 6, 2021. Witness 1 did not know ASBURY personally but was shown the Facebook video by an associate of ASBURY’s. Witness 1 provided ASBURY’s name and address to the FBI.

38. On January 17, 2021, FBI interviewed ASBURY at the address provided by Witness 1, which was ASBURY’s home. ASBURY admitted to attending the rally for President Trump and moving with the crowd to the Capitol building. ASBURY denied entering the Capitol or committing violence on January 6, 2021. ASBURY claimed he did not venture closer than 15 feet from the building but did witness violence towards law enforcement.

39. On March 23, 2021, the FBI interviewed another individual identified herein as “Witness 2.” Witness 2 had known ASBURY for approximately 30 years. Witness 2 stated that ASBURY posted on Facebook that he would be going to Washington D.C. on January 6, 2021. After the Capitol riot, Witness 2 viewed two videos posted by ASBURY on Facebook showing ASBURY cursing at law enforcement. The videos were removed from ASBURY’s Facebook shortly after January 6, 2021. Witness 2 also saw ASBURY’s photo on the FBI’s wanted list in connection to the Capitol riot. Witness 2 said ASBURY was wearing a tan Carhartt coat, which is consistent in description to the attire worn by ASBURY in surveillance footage of the Capitol during the January 6 riots, including the images contained in this Affidavit.

40. Using the information about ASBURY provided by Witness 1 and Witness 2, FBI queried DMV records as seen in **Image 1**. According to DMV records, ASBURY is approximately 43 years old, and his primary address is in Knoxville, Tennessee.



Image 1: DMV image of Michael ASBURY.

VIDEO FOOTAGE DEPICTING MICHAEL ASBURY

41. After receiving the tips regarding ASBURY's involvement, law enforcement reviewed numerous surveillance videos from the U.S. Capitol building and publicly available videos online. A man whose appearance is consistent with the person identified by Witness 1 and Witness 2 can be seen in the Lower West Terrace area of the Capitol building on January 6, 2021. Based on my training, experience, and my personal comparison of the video footage with ASBURY's Facebook posts, DMV records, and the information from Witness1 and Witness 2, the man seen in the video footage is ASBURY. ASBURY was initially seen wearing camouflage pants, a tan jacket, a camouflage backpack, and a camouflage balaclava with black trim along the face opening.

42. ASBURY was seen at the Capitol on January 6, 2021, in a publicly-available YouTube video⁴ entitled “Patriots STORM U.S. Capitol.” **Image 1** and **Image 2** are still images from said video.



FULL FOOTAGE: Patriots STORM U.S. Capitol (4K60fps)

Image 1: Still image from “Patriots STORM” video depicting ASBURY on Capitol grounds.

⁴ <https://www.youtube.com/watch?v=iNFcdpZdkh0> (Video 1)



Image 2: Still image from “Patriots STORM” video depicting ASBURY on the media tower on the west front of Capitol grounds.

43. A review of USCP surveillance footage, Washington, D.C., Metropolitan Police Department (MPD) body-worn camera (BWC) footage, open-source videos, and footage from other rioters revealed ASBURY repeatedly engaged in a violent obstructive conduct against multiple law enforcement officers inside the tunnel.

44. ASBURY was captured by Capitol building surveillance footage outside the tunnel entrance at approximately 2:49:25 pm. ASBURY entered the tunnel by climbing on the left archway, as seen in Image 4.



Image 3: Still image from Capitol building surveillance footage at 2:49:25 pm, depicting ASBURY at the entrance of the tunnel.

45. About one minute later, at 2:50:39 pm, ASBURY moved further into the tunnel. At this point, ASBURY appeared to lean his full body weight against the rioter in front of him (with no one pushing ASBURY from behind). Additional rioters joined behind him, pushing against him, and they collectively pushed together in a “heave-ho” effort against the police line until at about 2:51:20 pm. At that point, the mob appeared to have lost its momentum and dissipated backward, ASBURY among them.



Image 4: Still image from Capitol building surveillance footage at 2:50:39 pm, depicting ASBURY inside the tunnel participating in a heave-ho effort against the police line.

46. ASBURY re-entered the tunnel with the apparent intention to re-engage with the police line at approximately 2:53:19 pm. A rioter next to him sprayed toward the police line with OC spray. Another rioter directly behind him threw a large object toward the police line. ASBURY assisted in throwing a police shield toward the crowd behind him, away from the police line, as captured in Image 6 and Image 7. Other rioters followed suit, taking shields away from the police in an effort to disarm them.



Image 6: Still image from Capitol building surveillance footage at 2:53:30 pm, depicting ASBURY (red) at the mouth of the tunnel handing a police riot shield (blue) to the rioters behind him.



WASHINGTON
UNBELIEVABLE Footage | Trump Supporters Battle Cops Inside the Capitol

Image 7: Still image from the footage of journalist Jon Farina depicting ASBURY inside the tunnel holding a law enforcement shield over his head at approximately 2:53:30 pm. This appears to be a mirror image of 6.

47. BWC footage from MPD Sgt. William Bogner and Farina's footage depict ASBURY inside the vestibule doors of the tunnel around 2:56:41 pm, as depicted in **Image 8** and **Image 9**, respectively. Voices that appear to be from law enforcement officers are heard yelling, "Ladies and gentlemen, back up!" and "Get back!" while an alarm is sounding.



IMAGE 8: Still image from Sgt. Bogner's BWC footage depicting ASBURY at the police line inside the tunnel at 2:56:41 pm.



Image 9: Still image from Farina's footage depicting ASBURY and Sgt. Bogner inside the tunnel at approximately 2:56:41 pm. It appears to be a mirror-image of **Image 8**.

48. ASBURY began to make his way out of the tunnel at approximately 2:57:40 pm, after law enforcement sprayed OC spray toward the rioters. He removed the balaclava from his head as he exited.

49. At approximately 3:03:43, while ASBURY was inside the tunnel, the rioters initiated another heave-ho effort, their bodies moving in unison back and forth to apply force against the police line ahead. ASBURY again maneuvered his way to the front of the police line at approximately 3:04:07 pm, past the frame of the Capitol surveillance CCTV camera. However,

the footage of another rioter, Yvonne St. Cyr,⁵ captured him there. St. Cyr's video shows that ASBURY was inside of the doors leading into the building, where the police line was, as captured in **Image 10**. At the moment that ASBURY reached the front of the line, rioters behind him surged forward and began the back and forth heave-ho effort against the police. The video shows rioters with hands on each other's backs, pushing back and forth.

⁵ St. Cyr (D.D.C. Case No. 1:22-cr-185) was convicted at trial on March 10, 2023, of a total of six offenses, including two felony charges of interfering with a law enforcement officer during a civil disorder.



Image 10: Still image from St. Cyr's video depicting ASBURY beyond the doors to the Capitol building at approximately 3:04:07 pm.

50. ASBURY remained outside the tunnel until at least 3:41:55 pm.

ASBURY'S COMMUNICATION ACCOUNTS

51. As noted above, Witness 1 and Witness 2 reported a Facebook page associated with ASBURY. Based on my training and experience and the course of the investigation to date, your affiant believes the Facebook page reported by Witness 1 and Witness 2 is publicly identified by the URL facebook.com/Michael.Asbury.³¹ This was determined by comparing the publicly available Facebook images and videos to known images of ASBURY.

52. The FBI obtained the records associated with the above Facebook account. The records showed that ASBURY discussed his plans to travel to Washington, D.C., with Facebook Friend 1 (FF1) using Facebook's unified message feature, also known as a private message. On January 5, 2021, ASBURY sent a private message to FF1, "I'm headed to dc now." On January 6, 2021, FF1 sent ASBURY the following message: "Please tell me you're okay buddy." ASBURY responded at 7:34 pm, "I'm good brother. Just got out" and at 7:35 pm, "It was so fucking amazing i cant describe."

53. In public comments on January 7, 2021, ASBURY wrote, "I shook hands with the officer who peppered me. He seemed nice." "Btw, today wasn't about you. It was about our constitution." "We sent a fucking message today. You should be thanking us".

54. The Facebook account mentioned above listed a verified phone number to the account. The verified number matched that of the **Subject Device**, 865-765-2423. In multiple Facebook messages, ASBURY told other people his phone number and listed the number as 865-765-2423.

55. Phone number 865-765-2423 was carried by T-Mobile on January 6, 2021. Records provided by T-Mobile in August 2021 listed the subscriber for the account as a family member of ASBURY. The subscriber information also listed the following identifiers: MSISDN 8657652423,

IMEI Number 356694099258140. The IP address data sessions for the device with phone number 865-765-2423 placed the device in Washington DC on January 6, 2021.

56. The previously mentioned Facebook account, facebook.com/Michael.Asbury.31, was still active as of June 2023. The account name was listed as “Michael Asbury” and had publicly posted on May 12, 2023, about a band named “Wickid Garden” as seen in **Image 11**.



Image 11: Facebook post by ASBURY discussing a band, Wickid Garden.

57. I am aware that, as of June 2023, ASBURY is still using a device affiliated with phone number 865-765-2423. On June 21, 2023, FBI Special Agents conducted a ruse phone call

to 865-765-2423, the phone number associated with the **Subject Device**. ASBURY answered the call and confirmed he was Mike Asbury with a band called Wickid Garden.

PROPERTY TO SEARCHED

58. The property to be searched includes the **Subject Device**, a cellular telephone with the number 865-765-2423, with T-Mobile as the service provider, and with IMEI 356694099258140, or any successor cellular telephone which ASBURY obtained and is found in his possession.

59. There is probable cause to believe that ASBURY had in his possession a cellphone, also called an electronic device, while at the U.S. Capitol on January 6, 2021, since he was seen using said device in video footage, see **Image 12** below. The previously mentioned IP Address data session records provided by T-Mobile. There is probable cause to believe that ASBURY is still associated with the phone number 865-765-2423 due to the recent ruse call conducted by FBI Special Agents.



Image 12: Still image of ASBURY holding what appears to be a cell phone on Capitol grounds, on January 6, 2021. Based on my training and experience and my knowledge of this investigation to date, I recognize this as a restricted area, on which Asbury was not permitted.

COMPUTERS, ELECTRONIC STORAGE AND FORENSIC ANALYSIS

60. As described above, this Affidavit seeks permission to search for records that might be found, in whatever form they are found, to include the **Subject Device**. One form in which the records might be found is data stored on an electronic device or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

61. *Probable cause.* I submit that if an electronic device, such as the **Subject Device** or any successor device is found in ASBURY's possession, there is probable cause to believe those records will be stored on that electronic device or storage medium, for at least the following reasons:

a. As described in this Affidavit, ASBURY utilized an electronic device in restricted areas of the Capitol grounds on January 6, 2021. As mentioned previously, witness

interviews mentioned videos posted to Facebook by ASBURY shortly after January 6, 2021, that were subsequently deleted. The previously mentioned data session information provided by T-Mobile placed Asbury's device in Washington, DC, on January 6, 2021.

b. Based on my knowledge, training, and experience, it is common for individuals to back up or preserve copies of digital media (such as photos and videos) across multiple devices to prevent loss. Indeed, some companies provide services that seamlessly sync data across devices, such as Apple devices and the Apple iCloud service. Thus, there is reason to believe that evidence of the offense that originally resided on the **Subject's Device** may also be saved to any successor device found in ASBURY's possession. Moreover, here, as widely reported in the news media related to this matter, many individuals committing the **Target Offenses** kept and posted videos, photos, and commentary about their participation in these offenses, essentially bragging about their participation. Based on that, there is also probable cause to believe that evidence related to these offenses may have been transferred to and stored on digital devices beyond the particular digital device the Subject possessed during the offenses.

c. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded into a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

d. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the storage medium that is not currently being used by

an active file – for long periods of time before they are overwritten. In addition, an electronic device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

e. Wholly apart from user-generated files, electronic device storage media – in particular, electronic devices’ internal hard drive – contain electronic evidence of how an electronic device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Electronic device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

f. Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or “cache.”

62. *Forensic Evidence.* This Affidavit seeks permission to locate not only electronic device files that might serve as direct evidence of the crimes identified in the warrant, but also for forensic electronic evidence that establishes how electronic devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any electronic storage medium in ASBURY’s possession because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and

passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the electronic device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within an electronic device and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling law enforcement to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within an electronic device or electronic storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the electronic device or electronic storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the electronic device was remotely accessed, thus inculcating or exculpating the owner of the electronic device. Further, electronic device and storage media activity can indicate how and when the electronic device or storage media was accessed or used. For example, as described herein, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the electronic device accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some

information stored within an electronic device or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within an electronic device may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information within the electronic device may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how an electronic device works can, after examining this forensic evidence in its proper context, draw conclusions about how the devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the device and the application of knowledge about how a device

behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how an electronic device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

63. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of the storage media. Generally speaking, imaging is the taking of a complete electronic picture of the electronic device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how an electronic device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large amount of information. Reviewing that information for things described in the

warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements.* Electronic devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

64. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

65. *Biometric Unlocking.* Videos showed that ASBURY likely utilized a mobile device. I know from training, experience, and publicly available materials that mobile phones, like the **Subject Device**, often offer users the ability to unlock the device via biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint

scanners, facial recognition features, and/or iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

66. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

67. A user can register multiple fingerprints that can be used to unlock such a device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to a sensor on the device. In my training and experience, users often enable such biometric unlocking features because they are considered a convenient and secure method of unlocking a device. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the device.

68. In some circumstances, a biometric unlock function will not unlock a device even if enabled, and a passcode or password must be used instead. These circumstances can include: (1) devices that has been recently powered on or restarted, (2) devices that receive a remote locking command, (3) devices that have undergone a specified number of failed unlocking attempts (often five attempts), (4) devices that have not been unlocked within a specified period of time (often 48 hours) has passed since the last time the device was unlocked, and (5) devices that have not been unlocked via fingerprint unlock within a shortened specified time and the passcode or password

has not been entered in a recent period of days. Thus, in the event law enforcement encounters a locked device, the opportunity to unlock the device via biometric unlocking may exist only for a short time.

69. The passcode or password that would unlock the **Subject Device**, or any successor device found in ASBURY's possession is not known to law enforcement. Thus, it will likely be necessary to (1) press the finger(s) of the user(s) of these electronic devices to the device's fingerprint sensor; and/or (2) hold the device(s) in front of ASBURY's face with his eyes open to activate the facial-, iris-, and/or retina recognition feature in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock electronic devices with the use of the biometric unlock function of the user(s) is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

70. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock such devices via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the **Subject Device**, or any successor device found in ASBURY's possession, within the permitted number of attempts, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.


71. Due to the foregoing, I request that the Court authorize law enforcement to press ASBURY's fingers (including thumbs) to the fingerprint sensors and/or hold the device(s) in front of ASBURY's face with his eyes open to activate the facial-, iris-, and/or retina recognition feature of the **Subject Device**. Additionally, I request that the Court authorize law enforcement to press the fingers (including thumbs) of ASBURY to the fingerprint sensors and/or hold the device in

front of his face with his eyes open to activate the facial-, iris-, and/or retina recognition feature of electronic devices found in ASBURY's possession for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.

CONCLUSION

72. Based on the foregoing, I submit that this Affidavit supports probable cause for a warrant to search the **Subject Device** described in Attachments A; and seize the items described in Attachment B.

Respectfully submitted,



Jessi A. Mann
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on June 26th, 2023.



Hon. Jill E. McCook
United States Magistrate Judge

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
at KNOXVILLE

IN THE MATTER OF THE SEARCH OF:
A Mobile Device in the Custody or Control
of Michael Asbury

Case No. 3:23-mj-
Magistrate Judge

ATTACHMENT A

Property to Be Searched

The property to be searched includes a mobile telephone, bearing MSISDN: 8657652423, IMEI Number 356694099258140 and/or any successor cellphone bearing the phone number 865-765-2423 located on Michael ASBURY's person or otherwise within his custody or control.

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
at KNOXVILLE

IN THE MATTER OF THE SEARCH OF:
A Mobile Device in the Custody or Control
of Michael Asbury

Case No. 3:23-mj-
Magistrate Judge

ATTACHMENT B

Property to be seized

1. The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, relating to violations of 18 U.S.C. § 231(a)(3); 18 U.S.C. § 1752(a)(1) and (2); and Title 40 U.S.C. Section 5104(e)(2)(D)(F) (the “**Target Offenses**”) that have been committed by MICHAEL ASBURY and other identified and unidentified persons, as described in the search warrant Affidavit. including, but not limited:

- a. Evidence concerning planning to unlawfully enter the U.S. Capitol, including any maps or diagrams of the building or its internal offices;
- b. Evidence concerning unlawful entry into the U.S. Capitol, including any property of the U.S. Capitol;
- c. Evidence concerning awareness of the official proceeding that was to take place at Congress on January 6, 2021, i.e., the certification process of the 2020 Presidential Election;
- d. Evidence concerning efforts to disrupt the official proceeding that was to take place at Congress on January 6, 2021, i.e., the certification process of the 2020 Presidential Election;
- e. Evidence relating to a conspiracy to illegally enter and/or occupy the U.S. Capitol Building on or about January 6, 2021;

- f. Evidence concerning the breach and unlawful entry of the United States Capitol, and any conspiracy or plan to do so, on January 6, 2021;
 - g. Evidence concerning the riot and/or civil disorder at the United States Capitol on January 6, 2021;
 - h. Evidence concerning the assaults of federal officers/agents and efforts to impede such federal officers/agents in the performance of their duties the United States Capitol on January 6, 2021;
 - i. Evidence concerning damage to, or theft of, property at the United States Capitol on January 6, 2021;
 - j. Evidence of any conspiracy, planning, or preparation to commit those offenses;
 - k. Evidence concerning efforts after the fact to conceal evidence of those offenses, or to flee prosecution for the same;
 - l. Evidence concerning materials, devices, or tools that were used to unlawfully enter the U.S. Capitol by deceit or by force, including weapons and elements used to breach the building or to counter efforts by law-enforcement, such as pepper spray or smoke grenades;
 - m. Evidence of communication devices, including closed circuit radios or walkie-talkies, that could have been used by co-conspirators to communicate during the unlawful entry into the U.S. Capitol;
 - n. Evidence of the state of mind of the subject and/or other co-conspirators, e.g., intent, absence of mistake, or evidence indicating preparation or planning, or knowledge and experience, related to the criminal activity under investigation;
- and

- b. Any records, such as receipts for travel, which may serve to prove evidence of travel to or from Washington D.C. in January of 2021;
 - c. ASBURY's (and others') motive and intent for traveling to the U.S. Capitol on or about January 6, 2021;
 - d. ASBURY's (and others') activities in and around Washington, D.C., specifically the U.S. Capitol, on or about January 6, 2021;
- 4. Digital devices, including but not limited to, the **Subject Device**, used in the commission of, or to facilitate, the above described offenses, including taking pictures and or videos inside the Capitol Building while committing the **Target Offenses**;
- 5. For any digital device which is capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities as described in the search warrant Affidavit and above, hereinafter the **Subject Device**:
 - a. evidence of who used, owned, or controlled the **Subject Device** at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;
 - b. evidence of software, or the lack thereof, that would allow others to control the **Subject Device**, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the attachment to the **Subject Device** of other storage devices or similar containers for electronic evidence;

- d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the **Subject Device**;
- e. evidence of the times the **Subject Device** was used;
- f. passwords, encryption keys, and other access devices that may be necessary to access the **Subject Device** (noting that, as described below, this warrant does not compel ASBURY to state or otherwise provide any non-biometric password to the **Subject Device**);
- g. documentation and manuals that may be necessary to access the **Subject Device** or to conduct a forensic examination of the **Subject Device**;
- h. records of or information about Internet Protocol addresses used by the **Subject Device**;
- i. records of or information about the **Subject Device**'s Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

During the execution of the search of the **Subject Device** described in Attachment A, law enforcement personnel are also specifically authorized to obtain from ASBURY (but not any other individuals present at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock the **Subject Device** requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the **Subject Device**, to include pressing

fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition.

While attempting to unlock the **Subject Device** by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that the aforementioned person(s) state or otherwise provide the password or identify the specific biometric characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the **Subject Device**. Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) is permitted. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to the **Subject Device**, or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks the **Subject Device**, the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.